14-4

~~TOP SECRET~~

ARMY SECURITY AGENCY

120/50/TOPSEC/AS-14

Copy No. 6

From: CSGAS-14

To: AFSA 02A7

~~TOP SECRET~~

DF 187 B

120/49/TOPSEC/AFSA-14

THE CRYPTANALYTIC SUCCESSES OF OKW/CHI AFTER 1938

1. During his period of detention (September-December 1946) at the Hq 7707, European Command Intelligence Center, Oberursel, Germany, Wilhelm FENNER, former Ministerialrat as chief of cryptanalysis in the Armed Forces High Command Cryptologic Agency (OKW/Chi), wrote a lengthy report concerning his past career and his extensive experiences in the field of cryptology. This report was never issued in translation, although an inadequate summary by Army Security Agency was issued as TICOM/I-206.

2. It is presently planned to issue a complete translation of the entire report in the DF-series. The attached translation is the third of the series and is FENNER's description of the cryptanalytic successes of OKW/Chi after 1938. Pertinent German cryptologic terms with their explanation have been placed in the appendix.

Translated: EMP

December 1949

Distribution: Normal

35 copies

Copy No. ____

19 pages

TABLE OF CONTENTS

THE CRYPTANALYTIC SUCCESSES OF OKW/CHI AFTER 1938

A. Preliminary Remarks

My endeavor to give in answer to the third question of First Lieutenant MARY CHARLOTTE LANE[1] a statement of the cryptanalytic successes of OKW/Chi after 1938 is not free from the fear that some points will remain obscure in spite of the definitions and explanations given. The roots of-these obscurities lie in part in my inadequacy, because there are many details I never knew and just as many that I have forgotten; but they lie also in the fact that the cryptologists of the various countries work with very divergent concepts, and that the word an expression of the concept can occasion numerous misunderstandings. There are certainly some of my former colleagues in American custody. They might check, supplement, and improve upon my statements.

If I take the third question literally, that is to say, as if only purely cryptanalytical results were of interest, my account would leave gaps; I have no illustrative material whatsoever and answering such a question would be beyond my mental capacity. If, however, I combine the answer to this question with a description of the individual cryptographic systems which still stick in my memory, I believe I can give an account which can at least claim to be a comprehensive survey.

Out of portions of the ruins of the army and its staffs which collapsed in November 1918 the Cipher Section (Chi) of the German Ministry of War (Reichskriegsministeriums) was founded in 1920. In another place[2] I have already reported on its organization and development down to the collapse in May 1945. Therefore, the description of the cryptanalytic results from 1938 on concerns only a small part of the total results, but at the same time brings many supplemental details.

[1] Lt. LANE, then assigned to Hq ASA Europe, was the American officer who participated in the oral interrogations of FENNER (issued as TICOM/I-200) and who supervised the written interrogations here presented. The third question, to which reference is here made, concerned the cryptanalytic successes of OKW/Chi and FENNER's estimate of their relative importance.

[2] Second report of this series, DF-187A.

Everywhere, where cryptanalytic work was done, the principle was valid:

1. First look at the material carefully.

2. Consider what sort of a statistical count you will make.

3. Choose the appropriate form for your count or have a new form printed.

4. Try to gain from this count criteria for the recognition of the underlying cryptographic system.

5. Do not give an uncritical, free rein to your fancy.

6. Do nothing which is superfluous, and work systematically.

How often these rules were followed in individual cases cannot be stated. Indeed, no absolute boundary can be drawn between a recognition by cryptanalytic means and one achieved intuitively. With systematic work every solution is always obtained analytically, even if a plain French code is involved. And my entire unit worked systematically; there was no work by trial and error, much less by guessing; every assertion had to be justified - even doubts!

3. Cryptanalytic Successes of OKW/Chi by Country

Russia: From their first appearance to the summer of 1943 the cryptographic systems "OK" and their successors were worked on and solved. I think the first system of this kind was "OK-5". I am sure that OK-6 and OK-7 were solved and later, I believe, OK-8 as well. If I remember rightly, these were 4-digit codes with partial reencipherment by 2-digit substitution tables.

After some original copies were captured, solution become much simpler because now the entire vocabulary was known. Helsingfors successfully shared in the solution and in some cases finished more quickly than Chi. Work was also done on the NKVD system. However, I never saw any tangible results. My people (detailed to the Air Force) returned in the summer of 1943 and I never learned whether the Army and Air Force achieved any results later.

[illegible] the word was "yes". But I never saw any positive results. If solutions of this code with its infinite additive reencipherment were achieved, it was probably only when by error the infinite additive sequence had been used several times; otherwise, solution would have been impossible. For when blocks of additive were captured, it was clear that the blocks could not be used, to say nothing of the fact that they were not allowed to be used except in cases of catastrophe when no other systems were available.

As a matter of principle no work was done on the ciphers "Polgred", "Werkcindol", and other diplomatic systems because it was certain that the infinite additive sequence would not be repeated, and hence no basis for deduction could be found with even the most modern technical means. Moreover, it had to be assumed that the basic code was of a mixed-unit type.

Poland: Since the introduction of additive sequences as reencipherment for the diplomatic 4-digit code, Poland had in the course of years repeatedly improved its cryptographic systems. The digit sequences came to be forty digits long, later they were regularly a multiple of 4 plus 1 or 4 plus 3. E. g. L = 50 . 4 + 1 = 201. Hence the solution of such additive sequences depended exclusively on the amount of traffic. But while originally an infinite additive sequence (as I seem to recall) was valid for 14 days and was pretty sure to be used more than once - there were cryptographic clerks who would start using the additive at the same point in stereotype fashion - the infinite additive sequence was later replaced more frequently and was different for each circuit, e. g., Warsaw - Berlin, Warsaw - Washington; in fact, at the end, that is shortly before the war broke out, the infinite additive sequences on the link Warsaw - Berlin were different from those for traffic Berlin - Warsaw. And the changes occurred so rapidly that even when the code was well solved the telegrams could no longer be read because there would not even be two messages in the same key. Of the messages of the Government-in-Exile and of the Resistance Movement which appeared later, the majority were solved down to the middle of March. The extensive differences were derived mechanically. A second system of a more complex character I am no longer able to describe exactly. With great reservation I will say that substitution tables were used for these were seemingly non-systematic but still were interpreted as systematic according to certain laws of the group theory. The basic system was probably a so-called 2-digit substitution. I assume it to be known that the Poles had a first class contact with HITLER's Headquarters where they obtained pertinent stratetic information in good season. The cover number of this confidential agent was a 3-digit number (406[2]). In any case the chief men of OKW and of the German Government knew from the decipherment of Polish messages the demands for the cession of Pomerania as an ostensibly former Polish area, and likewise the report on the disappointments that the Soviet Russians were constantly causing the Poles after the German front was pushed back.

Czechoslovakia: No cryptograms appeared after the spring of 1939. Up to that time not a single government system had been solved. Apparently the basic syste was a letter substitution. The type of reencipherment was never learned. Parallel passages did not occur in the encrypted text. During the war Chi received isolated Czech cryptotexts of unknown origin but with the appropriate key. So far as I recall these were transpositions of a 2-digit substitution. The content dealt with contacts of some confidential agents.

Yugoslavia: The cryptographic systems of the Government-in-Exile were like the peacetime systems. They were read currently, with the natural interruption every time there was a change of code or of reencipherment. The actual system was a 5-letter code and a 2-letter substitution. However Yugoslavia always made the mistake of facilitating the analysis of its official telegrams; either the new code was nothing but a systematic shifting of the old one, e. g., by shifting the page numbers, or when a new code actually was used they continued to use substitution tables which had been solved. Even when the reencipherment changed daily telegrams were decrypted, provided there was enough traffic available. In any case the numerous variations of the system did not afford any sure protection against analysis. Yugoslavia offers a typical example of a cryptographic system which reduced the limit of its natural security by false use. If, at the beginning of the 40's, Yugoslavia had once introduced an absolutely new 5-digit code together with a new 2-letter substitution table and new variations, then with the rather scanty traffic not a single message would have [illegible] est variants of the reencipherment were complicated: they no longer replaced two adjacent digits of a line by two letters, but two digits one above the other, which were no longer from successive code groups. Thus, no longer:

12	45	67	89	29	23	45	56	71	45
ma	ro	sa	tu	pi	la	ro	bi	ni	ro

but

1 2 4 5 6	7 8 0 9 2
2 3 4 5 7 Kalafictca	8 0 1 6 0 ....

with numerous variations in the formation of pairs. Even though solution was facilitated by the above-mentioned aids, the work was not easy due to the pairing of heterogeneous groups of letters. With this type of reencipherment some 500 ten-letter groups were needed in order to reduce with certainty. Therefore, at the end, telegrams often remained unsolved. The content of the deciphered messages was always factual and therefore important.

Roumania: Roumania used for two decades with a persistence which was unique a system of 5-digit codes with substitution encipherment using simple digit substitution tables, e. g.

0 - 4
1 - 1
2 - 5
3 - 0
. . .

The idea that 10! - 1 different substitution tables are possible may have caused Bucharest to consider this cryptographic system secure, even though the solution of such a system was not difficult in and of itself because in spite of the reencipherment all the affinities were preserved (e. g., 13316 = 24429 = 90096) and a reduction to the basic code was always possible with enough traffic. Bucharest never failed to facilitate a break-in after a change of code by allowing the old and new codes to run parallel for a time because the more remote embassies had not yet received the new one so that now old and new codes were reenciphered with [illegible] ion tables. Or by oversight the reencipherment was forgotten when a new code was introduced; or one and the same text was enciphered in the old and in the new code. No other country ever exposed its cryptographic systems with such fatal precision! Not until 43/44 did Bucharest introduce a new system: 5-digit code reenciphered by infinite additive sequence. But even then Bucharest made the mistake of permitting multiple use of the very long additive sequence (as I recall it far over 5,000 digits), obviously because there was no opportunity of providing all embassies with adequate amounts of reencipherment material. And the additive was used several times! Now it was worth while to compute the differences although the difference catalogue contained several hundred thousand groups. Derivation was mechanical because such quantities of differences could never have been worked out by hand and mental arithmetic. This work, however, met with no success because the collapse of Roumania occurred, followed soon by the German collapse. The value of decrypted Roumanian messages varied with the degree of seriousness of the individual ambassadors.

The Military Attache system was interesting: a system of coupled transposition boxes; however I can no longer recall details now. The transposition boxes changed daily and the plain text was entered in the box complex in a definite order. This system brought extremely important information, as, for instance, the uncontrollable break-down of the Roumanian Army because of deficient supply of ammunition, equipment, and food.

France: The culminating point in the analysis of French cryptographic systems falls in the last period of peace, extending down to the capitulation of France. No other European country used such a multitude of cryptographic systems, of which frequently more than 12 were in use simultaneously. All systems which could not be immediately recognized by eye were differentiated by indicator groups (Kenngruppen marquants) which were introduced at a definite position in the encrypted text. Here belonged the majority of the plain 4-digit codes, each of which had a series of indicator groups. In practical work these were recognized without difficulty and were compiled in tables. Because of its structure and the poverty of diplomatic language, the solution of the 4-digit code itself caused no little difficulty - in any case it was not to be compared with the solution of the extensive codes of the Americans and English or with the grammatically difficult code books of the Poles. These plain codes formed the principal source of intelligence because the French used them without scruple for the transmission of important messages while they used reenciphered codes more rarely. As long as the French used dinome substitution tables for partial reencipherment of the 4-digit codes, solution was regularly possible if there was adequate material. For the unchanged portions of the otherwise reenciphered groups afforded an important criterion for solution. I am thinking here of the system with manifold variations, e. g.

0123 4567 8911 8213 4609 ....

where the connected digits were reenciphered with 2-digit substitution tables while those marked with an x remained unchanged, i. e., were parts of the elements of the basic code. When (during the war) the French reenciphered all pairs serially, it was no longer possible to get a solution; nothing absolute could be gained from the relativities even though the system at first sight appeared to be more primitive

0123 4567 8911 ....

At the moment I do not recall any other reencipherments.

When, after the capitulation of France, a demand was made that the French Government reveal certain codes, these codes had to be "deponiert" - hence the expression "code depose", France made almost no use of these cryptographic systems. France, you must know, was permitted free use of the Colonial system which had not been solved by Chi! Apparently it transmitted its most important Government traffic in this. The attempt to solve the system brought no success. Also de Gaulle's cryptographic system could not be solved.

Even before the military action with France began, the military systems of French higher staffs were solved. That was a 4- or 5-digit code which was systematically transposed (tableau carre). In the cryptograms a few short parallel passages (repetitions) were discovered. The interval between these parallel passages was constant and must therefore correspond to the width of the transposition box as cryptanalytic studies have shown. If I am not mistaken, the keys (Loesungen = Sch[illegible] [illegible] [illegible]tez the box itself were taken from the same code book. Despite all the cunning of this cryptographic system, the occurrence of short parallel passages proved fatal. By the aid of these deciphered messages tabs could be kept on the French Army far back into the homeland.

Belgium: Belgium used a letter code (5-letter ?) which was reenciphered by a substitution table connected with the date. As long as abundant traffic was available, solution of this system was successful but I no longer recall details. After the capitulation of Belgium only a few messages came in so that this source of information had little significance.

Netherlands: There was a reenciphered French code book. I no longer remember details. In some 20 years only two Belgian[3] diplomatic ciphers were solved.

Switzerland: Switzerland had German and French code books and also employed cryptographic machine systems (Enigma). The first two were solved. If I am not mistaken, there were several digit substitution tables for reencipherment in use at the same time; these were used to encipher portions of the intermediate text of equal length. I think I recall that some certain dinomes were replaced by a single digit. Our results were meager.

Egypt: Very rarely a plain French code appeared and this was solved.

Italy: For many years Italy used the system, 5-digit code reenciphered by 2-letter substitution table. Serious mistakes were made repeatedly. In these codes the entries were not distributed at random over the entire range of number 10^5 but whole blocks of 100 were blank, i. e., did not occur at all in the code. That was important when solving the reencipherment because "impossible" pairs could be eliminated. Substitution tables once used were not merely used again years later but the re-use was according to the calendar so that when such an already solved 2-letter substitution table appeared the analyst merely had to "decipher" the messages. If a new 5-digit code was introduced they did not use new tables simultaneously on all links so that the new system was soon compromised! This was so even during the war until Italy - already out on a feeble limb in a military way - introduced systems of the Impero type with Littoria reencipherment which Chi did not succeed in solving. The main reason was the sharp drop in traffic. I cannot give any de[illegible] regarding the type of the reencipherment: I should say additive sequences but I may be in error. I may be confusing this with some other system but I do know that Italy even used code groups of discarded codes as additive digits for reencipherment.

[3] FENNER presumably meant "Dutch" or "Netherland". [Translator's note].

England: During the course of years some 25 different cryptographic systems were observed and of these approximately 10 plain, non-alphabetic and non-systematic 5-letter codes of large size were solved. Solution depended entirel on the amount of material. The "Prodome messages", which probably were enciphered with an infinite digit series, were not worked on at all. The traffic receipts were extremely heavy during the war. But since the really important messages were sent in "Prodome", what we got that was useful, was relatively little. When London imposed a communications embargo before the landing of the Allies, there was actually a noticeable falling off in reporting from and to London. But even from messages of the other European diplomatic representatives not a single clue could be obtained as to place and time of the projected landings.

U. S. A.: The extraordinary "Brown" and "Grey" codes were solved. As in the case of England, solution depended entirely on the amount of traffic which at times came in enormous quantities. Both codes were available in the original in 1940 (?). On the other hand solution of cryptographic systems, the so-called ASEC 9 and ASEC 10, caused considerable difficulty. For the reencipherment of the one system 35 (?) strips were used, each bearing a different substitution alphabet; initially the sequence of the strips remained valid for a considerable time but later (1944 ?) they were so frequently permuted that solution could no longer be achieved. At the same time the number of strips was considerably increased, if I remember rightly. The original solution was not by analytic means. The break-in resulted on the basis of the code book supplied by Rome (?) and of tables made available by Budapest (?). Down to the battles before Tobruk, the reports of the U. S. military observer in Cairo were read and without doubt there [illegible] tactical significance for Field Marshal ROMMEL because the American reports regularly gave the movement of the English troops. The replacement of the system which then resulted was ostensibly due to the fact that some one in Rome talked about the successful analysis; in any event, something regarding this solution leaked through to unauthorized German officer circles in Italy. The fact that later on a solution of the problem could no longer be forced was due to the fact that, expressed mathematically, it was necessary in each case to solve an equation modulo 26.

The other cryptographic system consisted - I think - in the fact that a limited number of successive letters of the intermediate text had to be replaced by a substitution alphabet according to a table. I ask that you regard this statement very critically becausw I may have fallen into serious error because of the great number of very different systems. Perhaps, too, I am confusing these two systems with respect to their use in Cairo and with respect to the securing of documents from Rome and Budapest.

Denmark: Denmark used a plain letter (?) code the solution of which was easy. Infrequent messages and inconsequential content made it seem unimportant to work on them.

Norway: Norwegian systems were worked on only after the occupation. The work met with no success. In approximately four years hardly 200 messages were received.

Sweden: The very extensive 5-digit code caused many difficulties: after receipt of the complete code book from Rome (1940 ?) it was clear that the difficulties lay in the philological structure of the code: simultaneous use of Swedish, German, French, and English concepts. This had not merely confused the statistical studies so that nothing could be recognized and for a long time it was thought that some reencipherment was used which could not be attacked analytically, but greatly hindered the linguistic solution. Work on this system continued for months in a totally false direction! The mixture of languages was just as new and surprising as the code groups "repetition of the nth group" appearing in English systems after the First World War, groups which obviously could have a thousand different meanings in practice. Thus this code was a typical example of one cleverly constructed. The content of the few messages received was usually of no moment.

The bulk of the Swedish messages was enciphered by means of Hagelin's Teknik. However the "basket" of this device, i. e., the drum consisting of 25 (?) bars with the various riders was probably varied from message to message so that the almost infinite period of the system could not be pinned down. This problem was scheduled as the focal point of analytical studies, all the more since there was a rumor abroad that the USA was also beginning to use the Hagelin machine (1943/44 ?).

Spain, Portugal, Latin America: Work on Spanish diplomatic ciphers began to show progress in 1944 when Germany's collapse was already impending. I myself can give no details regarding this cipher. The Portuguese Government Code was available in the original. Whether it was enciphered or not I can no longer recall. Traffic came in very sparingly so that the results of cryptanalysis were full of gaps. The Brazilian system was solved completely and was available in the original. I think it was a 5-letter (?) code with some easy reencipherment, the type of which I no longer recall. Of other Latin-American countries the primitive systems of San Domingo, Ecuador, and Chile were occasionally solved but they were without any significance.

Hungary: The Hungarian system was worked on only occasionally and then not at all for years. The essential feature of the system was known: a digit code with numerous digit substitution tables which were used every time in a different sequence and with "skips" of different lengths. It was never possible to define the individual "skip lengths" and sift out "homogeneous" messages.

Turkey: The 5-digit codes were originally reenciphered by primitive substitution tables. The codes which were later introduced (from 1937 ? on) were systematically akin to their predecessors. At first similar codes were changed monthly, then short (20 place ?) reencipherment numbers were introduced, the solution of which did not cause the slightest difficulty. For Turkey again and again made the mistake of using known reencipherments with new codes. All the diplomatic ciphers - except that of the Ministry of the Interior - were solved. They afforded valuable information. Down to March 1945 some eight different codes were solved. England knew that the Turkish systems were poor and tried to force English systems on Turkey but Turkey did not fall for these!

Iran: Only a few very primitive cryptographic systems.

Greece: Greece sent few messages. Within my memory there were three different codes which were differentiated by an indicator in the third position of one of the first few groups, e. g., [illegible] . Whether they were reenciphered I no longer know.

Vatican: There were certainly two cryptographic systems. One of them was a plain code and was solved. However, it yielded only unimportant administrative matters. It occurred rarely. The reenciphered code was worked on for a time but then laid aside because the material was not adequate to permit of an unambiguous diagnosis.

Bulgaria: Essentially Bulgaria used a system consisting of a 5-digit code and a reencipherment in which the cryptotext group arose through transposition of the basic code group. Hence, when decrypting, the groups had to be "taken out" according to a variable scheme, e. g., instead of 12345-45312. Down to the time of the collapse some five such codes were solved currently. Bulgaria also made the mistake that an ostensibly new code really corresponded to its predecessor save that the ten digits underwent a certain considerably systematic change so that for instance from:

old 38 456 came new 599 36
old 28 556 came new 596 56

I think that once the row numbers were also changed in a similar fashion. The messages were often very informative!

Japan: Work was started only during the war. In spite of the numerous different systems which appeared, four plain codes in all were solved. The difficulty lay primarily in the not always unambiguous transcription of Japanese into Latin script. A transposition box with blank cells in the top row occasioned more work. We had as yet no experience in this field, and none with the structure of the telegraphic language. In working on this system successful use was made of the "bigram search device" (Bigrammsuchgeraet) mentioned in another place.[4] Once two vertical columns with a maximum of natural digraphs had been found, further solution ran along as a rule without difficulty. No other country had to send as many messages requesting checks and repetitions! Some 12 different

[4] In second of this series, DF-187A.

cryptographic systems were observed, but I am inclined to think that we had not yet succeeded in recognizing all kindred material. Messages usually without interest.

<u>China</u>: China was first monitored during the war and showed some 10 different cryptographic systems, of which three primitive ones were solved. Contents without value.

<u>Agents</u>: About the middle of 1944 I took over from the Army the work on numerous agent systems of France, Poland, the Balkans, and Italy. Most of these systems, all told some 60 were known, were based on the use of books or indicator words - key words. They used double transposition, transposed "Caesars", and also Caesars with one-time additive. I know of only one case in which solution of the system was successful <u>without</u> the previous arrest of the agent (Poland). Clarification of the radio networks alone meant little for the cryrtanalytic section. Most of the networks were intercepted; their number ran into the hundreds by the end of the war. But in 99 percent of all cases analysis came too late, namely after the arrest and after the capture of the key, if the net did not continue to operate with the now known key after the arrest was made. Since I had nothing to do with the agents myself and never came into contact with one, the SD (<u>Sicherheitsdienst</u> - Security Service) and the Counterintelligence (<u>Abwehr</u>) did as they saw fit. They worked from a point of view which I could not share: generally they stepped in and made arrests and, as a rule, caused the net to disappear; I was interested in monitoring the net, especially when I was able to solve the messages. Without ever having been able to get hold of precise documentation of the results of such arrests it is still my belief that the agent systems fulfilled their purpose admirably and that the service was very well organized.

C. Appraisal of Successes

Actual cryptanalysis: As an independent discipline actual cryptanalysis, though one of limited application, had repeatedly yielded good results (e. g., Polish systems, Roumanian additive, Japanese transposition), but it had not yet attained its full capacity. This work, even more than practical decipherment, calls for an environment free from disturbance (bombing attacks, smashed furniture, dirt, cold, and chronic undernourishment!). Since cryptology in view of the sometimes notably high status of cryptology in foreign countries had really become a science, one had to accept the fact that the fruits of cryptanalysis could only ripen slowly. The war period with its increasing dearth of personnel and material and with the burdening of the individual to the limit of his endurance was not favorable for such a development.

D. Conclusion

Thus OKW/Chi observed during the war and down to mid-March 1945 the encrypted telegrams of some 30 different countries. In the best period (down to the capitulation of France) the section put out as high as 3,000 messages a month. On the average three times as many were deciphered but not translated. Over a period of five years my unit received approximately 370,000 encrypted messages a year. The maximum number of colleagues, including all auxiliary workers, amounted to 250 persons (in the year 1942). From then on the number sank steadily because more and more men fit for military duty were withdrawn and because the President of the Labor Office in Berlin refused to assign to Chi the number of replacements requested. At the time of the capitulation I may still have had 120 persons.

There are perhaps three things with which the head of OKW can be reproached

1. With not having correctly evaluated the results of cryptanalysis or perhaps, granting correct evaluation, with not having properly utilized these results,

2. With having refused as unnecessary the decipherment of economic and commercial messages,

3. With not having kept my unit capable of performing its duties by transferring it promptly to his bomb-proof area.

I am of the opinion that these three mistakes were the direct consequence of the fateful doctrine of the Blitzkrieg and of the uncritical, erroneous belief in a miracle. However, God cannot be bribed and is therefore always on the side of the strongest battalions.

Wilhelm KEITEL 13.9.1946

[illegible]

Definition of Concepts and Explanations

By analysis of a cryptographic system (Geheimschriftanalyse) we understand recognition of the reencipherment (Ueberschluesselung) and of the basic system (Grundverfahren) of a secret text (Geheimtext) from criteria of its statistical study. Crudely expressed, the cryptanalytic solution of a secret text is the opposite of solution by guessing.

Cryptographic system (the actual "key" (Schluessel)) is the law (Gesetz) for the conversion of a plain text (Klartext) into a secret text (Geheimtext). Hence, secret text, (Geheimtext), secret message (Geheimspruch), cryptogram (Kryptogramm), encrypted message (Chiffrenspruch), crypt message (Chispruch), encrypted telegram (Chiffrentelegramm), crypt telegram (Chitelegramm), cipher text (Chiffrat), keyed message (Schluesselspruch), keyed text (Schluesseltext), enciphered message (verzifferter Spruch) are synonymous concepts without consistent consideration of the outward form of what is written.

To encrypt, encipher, key (verziffern, chiffrieren, schluesseln) is to convert according to the given law, i. e., according to the given cryptographic system, a plain text into a secret text.

To decrypt, decipher (entschluesseln, dechiffrieren) signifies the reverse operation. It leads to the deciphered message (Dechiffrat), plain text (Klartext), decrypted message (entschluesselten Spruch), telegram (Telegramm), etc.

To cryptanalyze, (entziffern, decryptieren) signifies, in contrast to the above, the conversion of a secret text into its plain text without authorized knowledge of the key.

[illegible] result of a regular deviation from the forms of expression of the written language. The task of the cryptanalytic section is to find this law.

A secret text, colloquially also a cryptographic system, is "derived" ("abgeleitet") from the plain text according to the law, i. e., the cipher rule (Schluesselregel). A cryptographic system is "solved" ("geloest"), likewine an encrypted telegram, etc.

Basic systems (Grundverfahren) are cryptographic systems which are derived by means of only one operation.

Reenciphered systems (Ueberschluesselte Verfahren) strictly speaking cryptographic systems derived by reencipherment, are encrypted texts (Chiffrate) which are derived by means of two or more operations.

Combined systems (Kombinierte Verfahren)are cryptographic systems which are derived by the successive use of two or more basic systems.

Independent reencipherments (selbstaendige Ueberschluesselungen) involve operational use of symbols which themselves are not cryptographic systems at all.

(1) Reencipherments by digit sequences (Zahlenreihen):

e. g. Plain text:	Answer to	your telegram	number
5-digit code as "intermediate text"	42577	29021	46396
Additive	42912	05967	39715
Secret text	84489	24988	75001

(2) Reencipherment by substitution table:

Substitution Table

0-3	5-2
1-6	6-5
2-0	7-8
3-1	8-4
4-9	9-2

e. g. Plain text:	Answer to	your telegram	number
[illegible]	42577	29021	46396
Secret text according to the table	90588	07306	95175

Page 18 MISSING

Size of a code (*Umfang eines Codes*) is the numerical area occupied by it. A code 0000-9999 using 4-digit groups has the size 10^4 or 10,000.

A code is mixed-unit (*wechselstellig*) if its code groups differ in length, consisting, for instance, of 3- or 4-letter groups.

Secret element (*Geheimelement*) is the component in the encrypted text corresponding to the plain-text concept, e. g., in a plain code text, the "code group".

Break-in (*Einbruch*). To achieve a break-in into a cryptographic system is to obtain a recognition of its regularity, generally associated with the initial stage of solution.

Every cryptographic system has its natural degree of security, its natural resistance to analysis, or its natural limit of resistance. If in the use of the system the limit of its resistance is reached or even exceeded, then the system becomes capable of solution.

It is the task of cryptanalysis to develop methods which will permit recognition of this limit value as early as possible with a minimum number of messages.

Cryptography is the science of encrypting, enciphering, encoding, (*verziffern, schluesseln, chiffrieren*) decrypting, deciphering (*dechiffrieren, entschluesseln*), etc. Cryptology is the science of the solution of a cryptographic system without (authorized) possession of the key.